Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at http://about.jstor.org/participate-jstor/individuals/early-journal-content.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

NOTE ON CUBIC EQUATIONS AND CONGRUENCES

L. E. Dickson

In the Annals for January, 1910, Mr. Escott has given certain cubic functions, for which the corresponding algebraic equations have either three* real roots or no real root, while the corresponding congruences have either three integral roots or no integral root. He did not, however, determine in what cases the roots of the congruences are integral and in what cases not integral. This problem will be treated here by two methods. Although the methods apply equally well to the other congruences, we restrict attention to that on page 90, which takes the following simpler form when x is replaced by $z-a$:

$$(1)\qquad z^3-2az^2+(2a-3)z+1\equiv 0 \qquad (\operatorname{mod} p).$$

In no case is $z=0$ or $z=1$ a root. Hence we may set

$$(2)\qquad 2a\equiv f(z)=\frac{z^3-3z+1}{z^2-z} \qquad (\operatorname{mod} p).$$

If y and z are roots of (1), then $f(z)=f(y)$. After clearing of fractions and factoring the resulting integral function, we get

$$(y-z)(yz-y+1)(yz-z+1)=0.$$

Hence the values of y are

$$(3)\qquad z,\quad \frac{1}{1-z},\quad \frac{z-1}{z}.$$

If any two of these are equal, then all three are equal and

$$(4)\qquad z^2-z+1=0.$$

The roots of (4) are $-\omega$ and $-\omega^2$, where $\omega=-\frac{1}{2}+\frac{1}{2}\sqrt{-3}$ is a cube root of unity. If $p=3$, the only case in which (1) has an integral root is $a\equiv 0$ and the root -1 is then a triple root. Next, let -3 be a quadratic non-residue of p. Then (4) has no integral root and the functions (3) are distinct. Hence the $p-2$ integers z, where $1 < z < p$, give in sets of three the same value to (2). Thus there are $\frac{1}{3}(p-2)$ values of $2a$ for which congruence (1) has three (distinct) integral roots and $\frac{1}{3}(2p+2)$ values for which it has no integral root. For example, if $p = 5$, it has integral roots (namely, 2, 3, 4) only when $2a \equiv 4$. Finally, let -3 be a quadratic residue of p. When z is a root of (4), $z^3 = -1$ and $2a = 3z$, so that $2a = -3\omega$ or $-3\omega^2$. The $p-4$ integers z, not roots of (4) and not 0 or 1, give in sets of three the same value to (2). Thus there are $2 + \frac{1}{3}(p-4)$, namely $\frac{1}{3}(p+2)$, congruences (1) having integral roots, and $\frac{1}{3}(2p-2)$ congruences (1) having no integral root. For $2a \equiv -3\omega$, (1) has the triple root $-\omega$. For example, if $p = 7$, it has the triple root 3 if $2a \equiv 2$, the triple root -2 if $2a \equiv 1$, the roots $-1, 2, 4$ if $2a \equiv -2$, but no integral roots in the remaining cases.

---

* It should be pointed out that the three roots may coincide and give a triple root.

The second method makes use of the criteria for the nature of the roots of a cubic congruence as developed elsewhere by the writer.* Let p be a prime > 3, and let R be the discriminant (product of squares of differences of the roots) of a cubic

$$y^3 + \beta y + b = 0. \tag{5}$$

The cubic congruence has a *single* integral root if, and only if, R is a quadratic non-residue of p; it has three distinct integral roots if, and only if, R is the residue of a square $81\mu^2 \neq 0$ and $e = \frac{1}{2}(-b + \mu\sqrt{-3})$ is the residue of the cube of a number $r + s\sqrt{-3}$ in which r and s are integers; it has no integral root if, and only if, R is a quadratic residue and e is not the residue of a cube.

To obtain the reduced form (5) of (1), set $z = y + \frac{2}{3}a$. Then

$$\beta = -\tfrac{1}{3}c, \qquad b = -\tfrac{1}{27}(4a-3)c, \qquad c = 4a^2 - 6a + 9,$$

$$R = -4\beta^3 - 27b^2 = c^2.$$

We may take $\mu = \frac{1}{9}c$. Then $27e = c(2a + 3\omega)$. Now

$$c = (2a + 3\omega)(2a + 3\omega^2).$$

If $2a$ is -3ω or $-3\omega^2$, (5) has the triple root $y = 0$. For the remaining values of $2a$,

$$e = \left(\frac{2a + 3\omega}{3}\right)^3 A, \qquad A = \frac{2a + 3\omega^2}{2a + 3\omega} \neq 0.$$

---

* *Bulletin of the American Mathematical Society*, vol. 13 (1906), p. 1.

Hence the problem is to determine the values of a for which A is a residue of a cube. Since $A \neq 1$, each A gives a definite value for $2a$.

First, let -3 be a quadratic residue of p. Then p is of the form $3l + 1$. Then A is the residue of a cube if, and only if, $A^l \equiv 1 \pmod{p}$, as shown by Fermat's theorem. There are $l - 1$ integral values of $A \neq 1$, and therefore $l - 1 = \frac{1}{3}(p - 4)$ values of $2a$. Incorporating the values -3ω, $-3\omega^2$, we conclude that there are in all $\frac{1}{3}(p + 2)$ values of $2a$ for which the congruence has three integral roots, including the two cases in which it has a triple root.

Next let -3 be a quadratic non-residue of p. Then p is of the form $3l - 1$. Since (4) is now irreducible modulo p, its roots $-\omega$ and $-\omega^2$ are Galois imaginaries and each is the p^{th} power of the other. To give a direct verification,

$$(-\omega)^p = -\omega^{3l-1} = -\omega^{-1}(\omega^3)^l = -\omega^2.$$

Hence $\omega^p = \omega^2$, so that $A^p = 1/A$. Thus $A^{p+1} = 1$. Now

$$(\rho + \sigma\omega)^{p^2} \equiv \rho + \sigma\omega \pmod{p},$$

when ρ and σ are integers. Hence if $A \neq 0$ is the cube of an expression $\rho + \sigma\omega$, we have

$$A^{\frac{1}{3}(p^2-1)} \equiv (\rho + \sigma\omega)^{p^2-1} \equiv 1 \pmod{p}.$$

But the greatest common divisor of $p + 1$ and $\frac{1}{3}(p^2 - 1)$ is now l. Hence the conditions are that $A^l \equiv 1$, $A \neq 1$. Thus there are $l - 1$ values of A and the same number for $2a$. The values -3ω, $-3\omega^2$ are now not integers. Hence the total number of values of $2a$ for which the congruence has three integral roots is $\frac{1}{3}(p - 2)$.

The results obtained by the two methods agree completely. The second method furnishes an explicit equation $A^l \equiv 1$ which is satisfied by the values of $2a$ yielding congruences with integral roots. To solve $A^l \equiv 1 \pmod{p}$, when $p = 3l + 1$, we have only to read off from a table of indices for the prime p the numbers A whose exponents are multiples of 3 (mod $p - 1$). For the case $p = 3l - 1$, we employ similarly a table* of indices for the Galois field of order p^2.

---

* Bussey, *Bulletin American Math. Society*, vol. 12, p. 21, vol. 16, p. 188.

The cubics obtained by Mr. Escott are included in the wider class of cubics whose discriminant is a perfect square. For any such cubic the roots are rational functions of a single root and the cubic admits of three linear fractional transformations into itself.† In the cubic discussed here these are defined by the functions (3).

THE UNIVERSITY OF CHICAGO,
JULY, 1910.

---

† Serret, *Algèbre supérieure*, vol. 2, pp. 466-469.